UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MASSACHUSETTS

LISA DIANE DANIELS, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. ANTHEM, INC., Defendant.	Case No. _____ Hon. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, Lisa Diane Daniels ("Plaintiff"), by counsel, on behalf of herself and all others similarly situated, hereby submits the following Class Action Complaint ("Complaint") against Anthem, Inc. ("Defendant") and upon personal knowledge as to her own acts and status, and upon information and belief, the investigation of her counsel, and the facts that are a matter of public record, as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Between approximately December 10, 2014 and January 27, 2015, Anthem, Inc. ("Anthem") was subject to one of the largest data breaches in history (the "Anthem data breach"), when hackers stole the personal and financial information of up to 80 million Anthem customers. The personal and financial information obtained by the hackers includes names, birthdates, Social Security numbers, street and email addresses, and employee data, including income.

2. Anthem failed to take adequate and reasonable measures to ensure its data systems were protected, failed to take available steps to prevent and stop the breach from ever happening, failed to disclose to its customers material facts, including that it did not have adequate computer systems and security practices to safeguard customers' financial account information and personal data, and failed to provide timely and adequate notice of the Anthem data breach. Anthem's conduct

has caused substantial consumer harm and injuries to millions of consumers across the United States.

3. As a result of the Anthem data breach, 80 million Anthem customers have been exposed to fraud and these 80 million customers have been harmed. As a direct result of the Anthem data breach, the proposed Class suffered the following injuries, including: theft of their personal and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Anthem data breach; the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal and financial information being placed in the hands of hackers; damages to and diminution in value of their personal and financial information entrusted to Anthem for the sole purpose of obtaining health insurance from Anthem and with the mutual understanding that Anthem would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; money paid to Anthem for health insurance during the period of the Anthem data breach in that Plaintiff and Class members would not have obtained insurance from Anthem had Anthem disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Anthem provided timely and accurate notice to them of the Anthem data breach; overpayments paid to Anthem for health insurance purchased during the Anthem data breach in that a portion of the price for insurance paid by Plaintiff and the Class to

Anthem was for the costs of Anthem providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Anthem did not do, and as a result, Plaintiff and members of the Class did not receive what they paid for and were overcharged by Anthem; and continued risk to their financial and personal information, which remains in the possession of Anthem and which is subject to further breaches so long as Anthem fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

4. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on behalf of herself and all similarly situated consumers whose account and/or personal identifying information was stolen as a result of the Anthem data breach. Plaintiff asserts claims against Anthem for violations of Massachusetts consumer laws, negligence, breach of implied contract, breach of Anthem's HIPAA Notice of Privacy Practices handbook, bailment, unjust enrichment, and invasion of privacy. On behalf of herself and all similarly situated consumers, Plaintiff seeks to recover damages, including actual and statutory damages, and equitable relief, restitution, disgorgement, costs, reasonable attorney fees, any other relief which the Court deems proper.

PARTIES

5. Plaintiff Lisa Diane Daniels is a United States Citizen and resides at 132 Franklin Street, 2ndFloor, Malden, Middlesex County, Massachusetts 02148. She is a current Anthem health insurance customer. Mrs. Daniels' personal, health, and financial information associated with her health insurance was compromised as a result of the Anthem data breach. Mrs. Daniels was harmed by having her financial and personal information compromised.

6. Plaintiff would not have given her personal and financial information to Anthem to purchase health insurance—indeed, she would not have obtained Anthem health insurance at all during the period of the Anthem data breach—had Anthem told her that it lacked adequate

computer systems and data security practices to safeguard customers' personal and financial information from theft, and had Anthem provided her with timely and accurate notice of the Anthem data breach.

7. Plaintiff suffered actual injury from having her financial, health, and personal information compromised and stolen as a result of the Anthem data breach.

8. Plaintiff suffered actual injury and damages in paying money to and purchasing insurance from Anthem during the Anthem data breach that she would not have paid had Anthem disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Anthem provided timely and accurate notice of the data breach.

9. Plaintiff was overcharged for health insurance purchased from Anthem during the Anthem data breach in that a portion of the purchase price included the costs of Anthem providing reasonable and adequate safeguards and data security measures to protect customers' financial and personal data, which Anthem failed to provide and, as a result, Plaintiff did not receive what she paid for and was overcharged.

10. Defendant Anthem, Inc. ("Anthem") is the second-largest health insurer in the United States. According to Anthem's own website, one-in-nine Americans receive coverage for their medical care through Anthem. Anthem is headquartered at 120 Monument Circle, Indianapolis, IN 46204.

JURISDICTION & VENUE

11. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class

are citizens of states different from the Defendant. Further, there is complete diversity of citizenship between Plaintiff, Lisa Diane Daniels, and Defendant. Defendant is incorporated and has its principal place of business outside of the state in which the Plaintiff resides.

12. Venue is proper within this district pursuant to 28 U.S.C. § 1391 because a substantial part of the acts and/or omissions giving rise to these claims occurred within this district. Plaintiff, Lisa Diane Daniels, is a resident of Middlesex County, Massachusetts and purchased Defendant's insurance in Middlesex County, Massachusetts.

CLASS ACTION ALLEGATIONS

13. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a) and 23(b)(3) are met with respect to the Class defined below.

14. The Plaintiff Class consists of all persons whose personal, financial, or health information was compromised by the data breach first disclosed by Anthem on February 4, 2015 ("Class Members").

15. The Class is so numerous that joinder of all members is impracticable. The Class includes approximately 80 million individuals whose personal, financial, or health information was compromised by the Anthem data breach. The precise number of members should be readily available from a review of Defendant's records.

16. There are numerous, common questions of both law and fact that predominate in the action over any questions affecting individual members. These common legal and factual questions, include, but are not limited to, the following:

a) whether Anthem engaged in the wrongful conduct alleged herein;

b) whether Anthem's conduct was deceptive, unfair, unconscionable and/or unlawful;

c) whether Anthem owed a duty to Plaintiff and members of the Class to adequately protect their personal, health, and financial information and to provide timely and accurate notice of the Anthem data breach to Plaintiff and members of the Class;

d) whether Anthem breached its duties to protect the personal, health, and financial information of Plaintiff and members of the Class by failing to provide adequate data security and whether Anthem breached its duty to provide timely and accurate notice to Plaintiff and members of the Class;

e) whether Anthem knew or should have known that its computer systems were vulnerable to attack;

f) whether Anthem's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of millions of consumers' personal, health, and financial data;

g) whether Anthem unlawfully failed to inform Plaintiff and members of the Class that it did not maintain computers and security practices adequate to reasonably safeguard customers' financial and personal data and whether Anthem failed to inform Plaintiff and members of the Class of the data breach in a timely and accurate manner;

h) whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of Anthem's conduct (or failure to act);

i) whether Plaintiff and members of the Class are entitled to recover damages;

j) whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

17. Plaintiff's claims are typical of the claims of the Class in that the representative Plaintiff, like all Class Members, had health insurance through Anthem and had their personal, health, and financial information compromised in the Anthem data breach, suffering harm.

18. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are qualified and experienced in class-action and complex litigation. Neither Plaintiff, nor her counsel, have interests that are adverse to, or in conflict with, other members of the Class.

19. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy.

20. The prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Anthem. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

21. The case will be manageable as a class action. Plaintiff and her counsel know of no unusual difficulties in the case and, upon information and belief, Defendant has computer systems that will allow the class, and damages issues in the case to be resolved with relative ease.

22. Because the elements of Rule 23 are satisfied in the case, class certification is appropriate. *Shady Grove Orthopedic Assoc., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 130 S. Ct. 1431, 1437 (2010) ("[b]y its terms [Rule 23] creates a categorical rule entitling a plaintiff whose suit meets the specified criteria to pursue her claim as a class action").

FACTS

The Healthcare Industry is Put on Notice of Cyber Attacks

23. Health care companies, like Anthem, have an obligation to maintain the security of their customers' personal, health, and financial information, which Anthem itself recognizes in its HIPAA Notice of Privacy Practices handbook where it acknowledges and addresses the consumers' "protected health information" or "PHI":

> We keep the health and financial information of our current and former members private, as required by law, accreditation standards and our rules.
>
> . . .
>
> We are dedicated to protecting your PHI, and have set up a number of policies and practices to help make sure your PHI is kept secure. We keep your oral, written and electronic PHI safe using physical, electronic, and procedural means. These safeguards following federal and state laws. Some of the ways we keep your PHI safe include securing offices that hold PHI, password Protecting computers, and locking storage areas and filing cabinets. . . .

24. The New York Times reports that "[t]he threat of a hacking is particularly acute in the health care and financial services industry, where companies routinely keep the most sensitive personal information about their customers on large databases." (http://www.nytimes.com/2015/02/05/business/ hackers-breached-data-of-millions-insurer-says.html (accessed Feb. 5, 2015)).

25. Indeed, on April 8, 2014, the FBI's Cyber Division issued a public Private Industry Notification titled "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain." The notification specifically cautioned that "[c]yber actors will

likely increase cyber intrusions against health care systems . . . due to . . . lax cybersecurity standards, and a higher financial payout for medical records in the black market."

26. The FBI cited a report issued in February 2014 by SANS, a leading computer forensics and security firm, warning:

> Health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property. . . . The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise.

27. By early 2014 computer breaches had become rampant in the healthcare industry, a fact widely disseminated inside and outside the healthcare sector. For example:

a) According to a Ponemon Institute report dated March 2013, 63% of the healthcare organizations surveyed reported a data breach during the previous two years. The majority of these breaches resulted in the theft of data. In a March 2014 report, the institute stated that criminal attacks on healthcare companies have increased 100% since 2010.

b) An EMC²/RSA White Paper published in 2013 indicated that during the first half of 2013, more than two million healthcare records were compromised, which was 31% of all reported data breaches.

c) According to the Identity Theft Resource Center, nearly half of all data breaches so far in 2014 have taken place in the healthcare sector.

d) According to a recent analysis of HHS data by the *Washington Post*'s "Wonkblog," the personal data of about 30.1 million people has been affected by 944 recorded "major" health data breaches (defined by HHS as one affecting at least 500 people) since federal reporting requirements under the 2009 economic stimulus package went into effect. This analysis did not include the CHS breach.

28. Several other studies have shown the healthcare industry to be one of the most affected by and least prepared to deal with hacking attempts. Despite the growing threat, the healthcare industry, and particularly companies like Anthem, has been slow to implement improved security measures – slower than other industries handling sensitive information, such as the retail

and financial sectors. For instance, the typical healthcare entity allocates only about 2 or 3 percent of its operating budget to its IT department, while retail and financial businesses devote more than 20 percent to IT. According to an annual security assessment conducted by the Healthcare Information and Management Systems Society, almost half of surveyed health systems said they spent 3 percent or less of their IT budgets on security.

The Anthem Data Breach

29. On February 4, 2015, Anthem, the second-largest insurer in the United States, made the following announcement by way of a letter from its President and CEO, Joseph R. Swedish, on its website:

> Anthem was the target of a very sophisticated external cyber attack. These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses and employment information, including income data. . . .
>
> . . .
>
> Anthem's own associates' personal information – including my own – was accessed during this security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data.
>
> Anthem will individually notify current and former members whose information has been accessed. . . .
>
> I want to personally apologize to each of you for what has happened, as I know you expect us to protect your information. We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Anthem.
>
> (http://www.anthemfacts.com/ (accessed Feb. 5, 2015)).

30. Anthem's website then stated that "all product lines are impacted" and the "impacted (plan/brand) include Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, Unicare, Healthlink, and DeCare." (http://www.anthemfacts.com/faq (accessed Feb. 5, 2015)).

31. Anthem notified the FBI of the breach and the FBI is investigating it.

32. Only as a result of the massive data breach, Anthem retained Mandiant, one of the world's leading cybersecurity firms, to evaluate Anthem's systems and identify solutions. (http://www.anthemfacts.com/ (accessed Feb. 5, 2015)).

33. The New York Times reported that "hackers were able to breach a database that contained as many as 80 million records of current and former customers, as well as employees." (http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html (accessed Feb. 5, 2015)).

34. The Anthem data breach "could be the largest breach of a health care company to date, and one of the largest ever of customer information." (*Id.*).

35. Anthem detected the breach on January 29, 2015, but did not publicly announce the breach until February 4, 2015.

36. As of the date of the filing of the complaint, individual affected customers still have not been personally notified by Anthem about the Anthem data breach.

37. Anthem "said it would begin notifying members in the coming weeks." (*Id.*).

38. The New York Times reports that Social Security numbers, which Anthem admits were obtained in the Anthem data breach, "are a particularly popular target for hackers. Combinations of Social Security numbers, birth dates and names sell for more than even credit card numbers in an increasingly sophisticated black market, where such information is sold and resold through popular auction sites." (*Id.*).

39. Anthem also admitted that the information involved was not encrypted in its database, which "drew immediate fire from some security experts" because "it is irresponsible for

businesses not to encrypt the data." (http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html#page=1 (accessed Feb. 5, 2015)).

40. This is not Anthem's first experience with data security breaches. As reported by the LA Times:

> In 2013, the company agreed to pay $1.7 million to resolve federal allegations that it exposed protected health information of 612,402 people online because of security weaknesses.
>
> Federal officials said Anthem had inadequate safeguards in an online application database and left names, birth dates, Social Security numbers and health data accessible to unauthorized people.
>
> The investigation by the U.S. Department of Health and Human Services found that the insurer didn't adequately implement policies for authorizing access to the database and didn't have technical safeguards in place to verify users.
>
> Anthem and other health insurers already suffer from a poor reputation for customer service and increasingly they must sell coverage directly to individuals as the federal health law reshapes the health insurance business.
>
> Analysts say Anthem will be under pressure to reassure consumers that it can be trusted with their sensitive information.

(*Id.*).

COUNT I – NEGLIGENCE

41. Plaintiff incorporates all paragraphs of this Complaint as if set forth herein.

42. Anthem owed a duty to Plaintiff and members of the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal, health, and financial information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Anthem's security systems to ensure that Plaintiff's and Class Members' personal, health, and financial information in Anthem's possession was adequately secured and protected.

Anthem further owed a duty to Plaintiff and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

43. Anthem owed a duty, as articulated in Anthem's HIPAA Notice of Privacy Practices handbook and otherwise, to protect its customers' sensitive financial, health, and personal information.

44. Anthem owed a duty to timely disclose the material fact that Anthem's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft and that it had been hacked in the past.

45. Anthem breached these duties by the conduct alleged in this Complaint by, including without limitation, (a) failing to protect its customers' personal, financial, and health information; (b) failing to maintain adequate computer systems and data security practices to safeguard customers' personal, health, and financial information; (c) failing to disclose the material fact that Anthem's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft; and (d) failing to disclose in a timely and accurate manner to Plaintiff and members of the Class, the material fact of the Anthem data breach.

46. The conduct alleged in the Complaint caused Plaintiff and Class Members to be exposed to fraud and be harmed. The injuries suffered by the Plaintiff and the proposed Class as a direct result of the Anthem data breach include: theft of their personal and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on

compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Anthem data breach; the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their personal and financial information being placed in the hands of hackers; damages to and diminution in value of their personal and financial information entrusted to Anthem for the sole purpose of obtaining health insurance from Anthem and with the mutual understanding that Anthem would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; money paid to Anthem for health insurance during the period of the Anthem data breach in that Plaintiff and Class Members would not have obtained insurance from Anthem had Anthem disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Anthem provided timely and accurate notice of the Anthem data breach; overpayments paid to Anthem for health insurance purchased during the Anthem data breach in that a portion of the price for insurance paid by Plaintiff and the Class to Anthem was for the costs of Anthem providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Anthem did not do, and as a result, Plaintiff and members of the Class did not receive what they paid for and were overcharged by Anthem; and continued risk to their financial and personal information, which remains in the possession of Anthem and which is subject to further breaches so long as Anthem fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

47. Anthem's actions were a substantial factor in bringing about the injuries and damages suffered by Plaintiff and Class Members.

48. Anthem knew or should have known that by not taking adequate precautions to protect Plaintiff's and Class Members' personal, health, and financial information Anthem was creating an unreasonable risk of harm and injury to Plaintiff and Class Members.

49. The injuries and damages alleged herein were the reasonably foreseeable result of Anthem's conduct.

50. Had Anthem undertaken the appropriate precautions, safeguards, and steps described herein, the injuries and damages complained of here would not have occurred.

51. As a direct and proximate result of Anthem's conduct and omissions described above, Plaintiff and proposed Class Members suffered harm and damages as described herein.

COUNT II – BREACH OF IMPLIED CONTRACT

52. Plaintiff incorporates all paragraphs of this Complaint as if set forth herein.

53. When Plaintiff and members of the Class provided their financial, health, and personal information to Anthem in order to purchase health insurance from Anthem, Plaintiff and members of the Class entered into implied contracts with Anthem pursuant to which Anthem agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

54. Anthem represented to Plaintiff and Class Members that it protected its customers' personal, financial, and health information. Anthem also represented that it would timely and accurately notify Plaintiff and Class Members if their data was breached and/or compromised. Plaintiff and Class Members relied on this representation when making the decision to purchase health insurance from Anthem and provide Anthem with personal and financial information.

55. Anthem benefited from this implied contract by obtaining payment from Plaintiff and Class Members for health insurance. Plaintiff and Class members expected Anthem safeguard

their personal, health and financial information from disclosure to unauthorized individuals or entities and expected Anthem to timely notify them that their data had been breached and compromised.

56. Plaintiff and Class Members would not have provided and entrusted their financial, health, and personal information to Anthem in order to purchase health insurance from Anthem in the absence of the implied contract between them and Anthem.

57. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Anthem.

58. Anthem breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the personal, health, and financial information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of Anthem data breach.

59. The losses and damages sustained by Plaintiff and Class Members as described herein were the direct and proximate result of Anthem's breaches of the implied contracts between Anthem and Plaintiff and members of the Class.

COUNT III – BREACH OF CONTRACT

60. Plaintiff incorporates all paragraphs of this Complaint as if set forth herein.

61. Anthem has a contractual obligation to maintain the security of its customers' personal, health, and financial information, which Anthem itself recognizes in its HIPAA Notice of Privacy Practices handbook where it addresses the consumers "protected health information" or "PHI":

> We keep the health and financial information of our current and former members private, as required by law, accreditation standards and our rules.
>
> . . .

> We are dedicated to protecting your PHI, and have set up a number of policies and practices to help make sure your PHI is kept secure. We keep your oral, written and electronic PHI safe using physical, electronic, and procedural means. These safeguards following federal and state laws. Some of the ways we keep your PHI safe include securing offices that hold PHI, password Protecting computers, and locking storage areas and filing cabinets. . . .

62. Anthem breached that contractual obligation by failing to safeguard and protect the personal, health, and financial information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of Anthem data breach.

63. Had Anthem fully performed its contractual obligation to take appropriate precautions, safeguards, and steps described herein, the injuries and damages complained of here would not have occurred.

64. The losses and damages sustained by Plaintiff and Class Members as described herein were the direct and proximate result of Anthem's breaches of the contracts between Anthem and Plaintiff and members of the Class.

COUNT IV – BAILMENT

65. Plaintiff incorporates all paragraphs of this Complaint as if set forth herein.

66. Plaintiff and the Class delivered their personal, health, and financial information to Anthem for the exclusive purpose of obtaining health insurance from Anthem.

67. In delivering their personal and financial information to Anthem, Plaintiff and Class members intended and understood that Anthem would adequately safeguard their personal and financial information.

68. Anthem accepted possession of Plaintiff's and Class Members' personal, health, and financial information for the purpose of providing health insurance to Plaintiff and Class Members.

69. Anthem did in fact use Plaintiff's and Class Members' personal, health, and financial information for the purpose of providing health insurance to Plaintiff and Class Members.

70. By accepting possession of Plaintiff's and Class Members' personal, health, and financial information, Anthem understood that Plaintiff and Class Members expected Anthem to adequately safeguard their personal, health, and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

71. During the bailment (or deposit), Anthem owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their personal, health, and financial information.

72. Anthem breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' personal, health, and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class Members' personal, health, and financial information.

73. Anthem further breached its duty to safeguard Plaintiff's and Class Members' personal, health, and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the Anthem data breach.

74. The losses and damages sustained by Plaintiff and Class Members as described herein were the direct and proximate result of Anthem's breach of the duty owed to Plaintiff and members of the Class.

COUNT V –

VIOLATIONS[1] OF M.G.L. c. 93A, REGULATION OF BUSINESS PRACTICES FOR

[1] Plaintiff is in the process of providing written notice under M.G.L. c. 93A, however 30 days has not yet passed. Therefore, Plaintiff will amend to add a specific reference to a violation of M.G.L. c. 93A once the required timeframe has passed.

CONSUMER PROTECTION ACT

75. Plaintiff incorporates all paragraphs of this Complaint as if set forth herein.

76. Anthem engaged in trade and commerce within the Commonwealth of Massachusetts.

77. As described herein, Anthem represented that it had taken adequate steps to safeguard consumer's personal and financial information when in fact it did not take adequate steps.

78. As described herein, Anthem failed to accurately disclose all material information before Plaintiff and Class Members transacted to purchase Defendant's insurance.

79. Anthem's willful and knowing withholding of important information about the inadequate security measures taken to protect Plaintiff's and Class Members personal, health, and financial information and Anthem's withholding of the material facts surrounding the data breach constitute a violation of M.G.L. c. 93A.

80. Anthem actively, knowingly, and deceptively misrepresented to Plaintiff and Class Members that Anthem took appropriate precautions to safeguard Plaintiff's personal and financial information. This conduct evidences bad faith and unfair and deceptive practices.

81. Anthem engaged in the conduct as described herein that created a likelihood of confusion and misunderstanding.

82. Anthem willfully, wantonly, and knowingly engaged in the conduct described herein, which they knew was deceptive, in the course of business, trade and commerce, and had a deleterious impact on the public interest.

83. Anthem's willful and knowing failure to utilize adequate security measures to protect Plaintiff's and Class Members personal, health, and financial information, in all likelihood, to save Anthem costs, where it knew or should have known that the healthcare industry was a target

for hackers, constitutes a violation of M.G.L. c. 93A.

84. Anthem's conduct as described herein constituted unfair and deceptive acts and practices, including, but not limited to:

a) representing that Anthem protected its customers' personal, financial, and health information;

b) failing to maintain adequate computer systems and data security practices to safeguard customers' personal, health, and financial information;

c) failing to disclose the material fact that Anthem's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, and

d) failing to disclose in a timely and accurate manner to Plaintiff and members of the Class the material facts of the Anthem data breach.

85. Plaintiff and Class Members relied on Anthem's representations.

86. The practices described herein are unfair because they offend public policy as established by statutes, the common law, or otherwise. Additionally they were unethical and unscrupulous, and caused substantial injury to consumers including Plaintiff and Class Members. Anthem engaged in an unconscionable course of action.

87. Anthem is liable to Plaintiff and Class Members for all statutory, direct and consequential damages, fees and costs, resulting from this breach, including multiple damages, and any other relief which the Court deems proper.

COUNT VI – UNJUST ENRICHMENT

88. Plaintiff incorporates all paragraphs of this Complaint as if set forth herein.

89. Plaintiff and Class Members conferred a monetary benefit on Anthem in the form of monies paid for the purchase of health insurance from Anthem during the period of the Anthem data breach.

90. The monies paid by the Plaintiff and Class Members were supposed to be used by Anthem, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

91. Plaintiff and Class Members reasonably expected the monies paid to Anthem to be used in that way.

92. Anthem failed to provide reasonable security, safeguards, and protections to the personal, health, and financial information of Plaintiff and Class Members, in all likelihood, to save Anthem costs, where it knew or should have known that the healthcare industry was a target for hackers, and as a result the Plaintiff and Class Members overpaid Anthem for the health insurance they purchased.

93. Under principles of equity and good conscience, Anthem should not be permitted to retain the money belonging to Plaintiff and Class Members because Anthem failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' personal, health, and financial information that they paid for but did not receive so that Anthem is ultimately unjustly enriched.

94. Anthem wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

95. Anthem's enrichment at the expense of Plaintiff and Class Members is and was unjust.

96. As a result of Anthem's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Anthem, plus attorneys' fees, costs, and interest thereon.

COUNT VII – INVASION OF PRIVACY, M.G.L. 214 § 1B

97. Plaintiff incorporates all paragraphs of this Complaint as if set forth herein.

98. Plaintiff and Class Members supplied Anthem with sensitive and private personal, health, and financial information with the purpose of obtaining health insurance.

99. Anthem had a duty to protect and safeguard Plaintiff's and Class Members' private information.

100. Anthem represented to Plaintiff and Class Members that it would protect and safeguard the private information supplied by Plaintiffs and Class Members as described herein.

101. Plaintiff and Class Members reasonably relied on the representations made by Anthem that their private information would not be disseminated to unauthorized individuals or entities.

102. Anthem breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' personal, health, and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class Members' personal, health, and financial information.

103. The dissemination of Plaintiff's and Class Members' private and personal information constitutes substantial and serious interference with their privacy under M.G.L. 214 § 1B.

104. As a direct and proximate result of the dissemination of Plaintiff's and Class Members' information, they have suffered severe mental or emotional distress in addition to potential future financial distress.

105. As a result of Anthem's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to monetary damages plus attorneys' fees, costs, and interest thereon, and any other relief which the Court deems proper.

RELIEF REQUESTED

Plaintiff, on behalf of herself and all others similarly situated, requests that the Court enter judgment against Anthem, as follows:

1. Certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure;

2. Ordering Defendant to disclose in computer format, or in print if no computer readable format is available, the names and addresses of all those individuals who are similarly situated, and permitting Plaintiff to send notice of this action to all those similarly situated individuals including the publishing of notice in a manner that is reasonably calculated to apprise the potential class members of their rights under this litigation;

3. Designating the Named-Plaintiff to act as the Class Representative on behalf of all similarly situated individuals;

4. An award to Plaintiff and the Class of compensatory, direct, consequential, statutory, and incidental damages;

5. An award of attorneys' fees, costs, and expenses, as provided by law, or equity, or as otherwise available;

6. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

7. Such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Dated: February 24, 2015

Respectfully submitted,

PLAINTIFF LISA DIANE DANIELS, Individually and on Behalf of All Others Similarly Situated,

/s/ Lisa Lee

Lisa Lee, BBO# 684631
Janet, Jenner & Suggs, LLC
31 St. James Avenue, Suite 365
Boston, Massachusetts 02116
Phone: (617) 933-1265
Fax: (410) 653-9030
Email: llee@MyAdvocates.com

Robert K. Jenner (*pro hac vice* to be filed)
Justin A. Browne (*pro hac vice* to be filed)
Janet, Jenner & Suggs, LLC
Commerce Centre East
1777 Reisterstown Road, Suite 165
Baltimore, Maryland 21208
Phone: (410) 653-3200
Fax: (410) 653-9030
Email: rjenner@MyAdvocates.com
Email: jbrowne@MyAdvocates.com

Counsel for Plaintiff and the Proposed Plaintiff Class Members